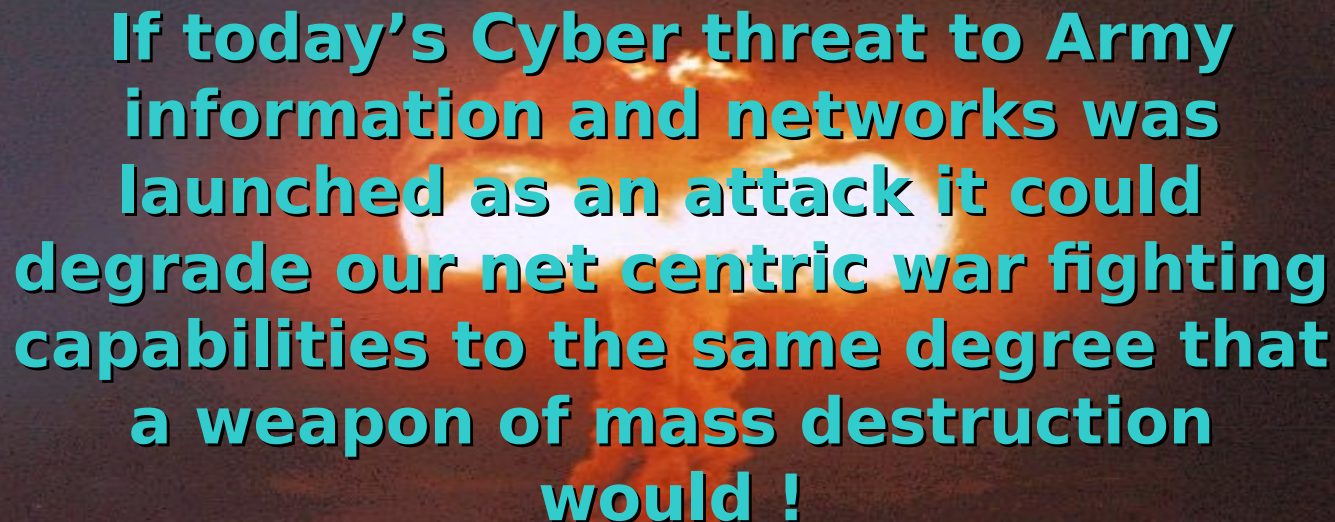


North Central CPOC PSM/DOIM Conference



Information Assurance
May 19, 2004

Information Assurance - Key to Information Superiority



**If today's Cyber threat to Army
information and networks was
launched as an attack it could
degrade our net centric war fighting
capabilities to the same degree that
a weapon of mass destruction
would !**

**The reconnaissance phase of a
Cyber war is**

Wednesday, May 19, 20

North Central CPOC

The Cyber War

- The average computer is being scanned or probed 23 minutes after it comes online.
- We are attacked and defend against those attacks on a daily basis.
- Less than 2% of the attacks are successful.



Information Assurance

- System/Data Security Practices
- Information Assurance Vulnerability Management
- Virus Protections

System/Data Security Practices

“The National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems.”

- General Accounting Office

(26 Jul 00)



System/Data Security Practices

- Physical Security
- System Documentation
- Hardware/Software Maintenance
- Security Awareness Training
- Incident Response

Physical Security

- A system is only as safe as the physical safeguards implemented to protect it.
 - Physically secure systems against intrusion
 - Lock screens when leaving work area
 - Screensaver time setting and password protection
 - Unauthorized devices



System Documentation

- Know what you have:
 - Hardware
 - Software
 - Configuration
- If you do not know what your system should look like it can be very difficult to identify hostile additions.

Hardware/Software Maintenance

- Hardware with vulnerabilities should be upgraded or replaced.
- Software should be patched to remediate security vulnerabilities.
 - Information Assurance Vulnerability Alerts (IAVAs)

Security Awareness Training

- Knowledge is the best defense
 - User responsibilities
 - What constitutes an attack?
 - Social Engineering Attacks
- AR25-2 mandates user training **before** issuance of a password for network access and annual refresher training
- Online user training available at <http://ia.gordon.army.mil>

Incident Response

- At a minimum, users must inform their Information Assurance Security Officer of any suspicious activity.
- In most cases, infected/compromised machines must be disconnected from the network and rebuilt.
- Systems Administrators and Security Officers must follow other reporting requirements mandated by AR25-2.

Information Assurance Vulnerability Management

“At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information tools and techniques.”

- Defense Science Board, 2001



Information Assurance Vulnerability Management (IAVM)

- IAVM compliance is the ***absolute minimum*** standard for all information systems...not a preferred state. (AR25-2, Section IX, Para 4-24a)
- A proactive methodology of maintaining, patching, and updating systems before exploitation.

IAVM Phases

1. Vulnerability identification, dissemination and acknowledgement
2. Application of measures to affected systems to make them compliant
3. Compliance reporting
4. Compliance verification

Army Implementation of IAVM

- Army Computer Emergency Response Team (ACERT) is the Army focal point for initiation of the IAVM process (<https://www.acert.1stiocmd.army.mil/index.htm>)
- Vulnerability identification and dissemination is handled at this level

Vulnerability Acknowledgement

- IAVM Messages issued by ACERT
 - Information Assurance Vulnerability Alert (IAVA)
 - Information Assurance Vulnerability Bulletin (IAVB)
 - Information Assurance Technical Tip (IATT)
- Messages must be acknowledged in Compliance Reporting Database v2 (CRD2) (<https://newia.us.army.mil>)

Vulnerability Mitigation & Compliance Reporting

- Actions specified in IAVM notices ***must*** be implemented by the indicated suspense
- Compliance must be reported in CRD2
- Harris STAT Scanner is the tool approved by the Army for use in verifying IAVM compliance

Compliance Verification

- IAVA Compliance Verification Teams (CVTs) will conduct short-notice inspections of randomly selected units to verify compliance with IAVM messages.

Virus Protections

“Cyber attacks can be conceived and planned without detectable logistical preparation...they can be clandestinely rehearsed, and then mounted in a matter of minutes or even seconds...”

**President's Commission on
Critical Infrastructure Protection, Oct
97**



Army Policy

- Army policy requires the installation of DoD approved anti-virus software on all Army systems
- Virus definitions must be updated ***at least*** every two weeks
- Software and current policy are available at the ACERT web site:
(<https://www.acert.1stiocmd.army.mil/index.htm>)

May 12, 2004

Crackers Delcare Cyberware on USA

<http://www.zone-h.org/en/news/read/id=4225>

Siegfried www.zone-h.org admin
05/12/2004

Famous Brazilian newspapers have been informed that a new hacking group composed of worldwide individuals (from Brazil, China, Hong Kong and Russia) has declared cyberwar on the United States of America.

Its name is Hackers Against America (HAA) and their web site is hosted on a Russian server. According to what is written on the main page, they plan to integrate new members and launch attacks against computers based in the US (cracking some of them but also use worms, viruses) in order to steal private documents. Some samples of documents and codes are available on the web site, although they don't seem to be secret at all and possible to find by using search engines.

Even if this threat appears to be tiny now, it is probably not a hoax and it could grow in the future, just keep an eye on it.

João Magalhães from www.estadao.com.br contributed to this article

Information Assurance

*“ In the near future, **information warfare will control the form and future of war...** Our sights must not be fixed on the fire-power of the industrial age; rather, they must be trained on the information warfare of the information age. ”*

-- Major General Wang Pufeng

Wednesday, May 19, 20

North Central CPOC

Peoples Liberation Army China

Information Assurance Web Sites

- Army Information Assurance
 - <https://informationassurance.us.army.mil>
- Army Computer Emergency Response Team
 - <https://www.acert.1stiocmd.army.mil/index.htm>
- DoD Computer Emergency Response Team
 - <http://www.cert.mil/>
- Compliance Reporting Database
 - <https://newia.us.army.mil/>
- Army IA Virtual Training
 - <https://iatraining.us.army.mil/>

Information Assurance Web Sites

- School of Information Technology – Fort Gordon
 - <https://ia.gordon.army.mil>
- Information Assurance Support Environment
 - <http://iase.disa.mil/>
- Microsoft Security Home Page
 - <http://www.microsoft.com/security>
- SecurityFocus
 - <http://www.securityfocus.com/>